

Appl. No. 09/903,991

Reply to Office Action of: June 22, 2005

**BEST AVAILABLE COPY****REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant advises that a Change of Correspondence Address form was filed on April 4, 2005. However, the Office Action dated June 22, 2005 was mailed to the previous address of Applicant's representative. Applicant requests that the Office update its records to effect the change of address, as well as amend the Attorney Docket number as indicated above.

**Amendments to the Specification**

The specification is amended on page 4 to remove the embedded hyperlinks as requested by the Examiner.

**Amendments to the Claims**

Claim 1 is amended to clarify the wording of step a) and to correct typographical errors. Claim 13 is amended to correct a typographical error. No new matter is believed to have been added by way of these amendments.

**Claim Rejections – 35 U.S.C. §102**

Claims 1, 4 and 12-19 have been rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,832,322 to Boden et al. Applicant respectfully traverses the rejections as follows.

The present application relates to systems and method for resolving a web site address when connected with a virtual private network. Claim 1, in part, requires that a software module monitor and intercept domain name requests from a public host when the public host is connected to a virtual private network (VPN). In order to "fool" the domain name server (DNS) of the public host, the software module modifies the request and sends it to a DNS for the VPN. The public host thinks that it is requesting an address location from the internet service provider (ISP) DNS, but the software module modifies the request so that the public host can request an address that is located within the VPN, without being altered or programmed to do so.

The DNS of the VPN resolves the request and returns an address location to the software module as a domain name response. The response is modified so that the public host believes

Appl. No. 09/903,991

Reply to Office Action of: June 22, 2005

**BEST AVAILABLE COPY**

the address was resolved by the ISP DNS, and is provided for use by the public host (see the example set forth on page 5, lines 15-26 and page 6, lines 12-25).

Boden teaches a system for integrating network address translation (NAT) with internet protocol (IP) security. Security is provided in a VPN by performing one or a combination of four types of VPN NAT. This procedure involves dynamically generating NAT rules and associating them with the manual or dynamically generated security associations before beginning IP security that uses the security associations. As IP Sec is performed on outbound and inbound datagrams, the NAT function is also performed.

Boden does teach modifying IP addresses in order to perform NAT. However, Boden does not teach having a software module monitor, intercept and modify domain name requests so that a request made by a public host that is intended for an ISP DNS, is rerouted to a VPN DNS, without the public host being aware of or being configured to do so. The Examiner relies on Figure 2 and column 6, line 60 to column 7, line 36 of Boden in rejecting claim 1.

In Figure 2 the host communicates with the DNS of the VPN gateway directly, and the VPN gateway performs NAT before forwarding IP addresses to the other VPN gateway. Figure 2 does not show a software module intercepting a request between the host and the DNS. The host intentionally sends the request directly to the DNS, where the VPN gateway then performs NAT. This is quite contrary to what is recited in claim 1. Boden does not enable the public host to be "fooled" into making requests to a VPN. The arrangement shown in Figure 2 clearly indicates that Boden intends to communicate directly with the VPN gateway.

Accordingly, Boden does not teach a software module monitoring and intercepting requests, then modifying the requests and routing the requests to a DNS. In fact, Boden teaches quite the opposite, namely, the host intends to send requests directly to the DNS and thus cannot perform the operations of claim 1, particularly wherein the host is "fooled" into believing that they are corresponding with the ISP of the DNS. Therefore, Boden does not teach every element of claim 1, and as such cannot anticipate.

Claims 4 and 12-16 are either directly or indirectly dependent on claim 1, and as such are also believed to distinguish over Boden.

Claim 17 is directed to a system that in part includes a software module that performs operations similar to those recited in claim 1. Therefore the above remarks with respect to claim 1, equally apply to claim 17. Claims 18 and 19 are dependent on claim 17, and as such are also

Appl. No. 09/903,991

Reply to Office Action of: June 22, 2005

**BEST AVAILABLE COPY**

believed to distinguish over Boden.

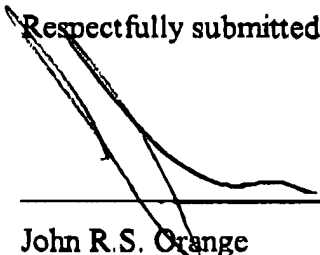
**Summary**

In view of the foregoing, Applicant respectfully submits that claims 1, 4 and 12-19 clearly and patentably distinguish over Boden, and are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

The Examiner is invited to contact the undersigned to discuss the present application in view of the finality of the rejections.

Respectfully submitted,



---

John R.S. Orange  
Agent for Applicant  
Registration No. 29,725

Date: October 24, 2005

BLAKE, CASSELS & GRAYDON LLP  
Suite 2800, P.O. Box 25  
199 Bay Street, Commerce Court West  
Toronto, Ontario M5L 1A9  
CANADA

Tel: 416.863.3164  
JRO/BSL